Tijd voor Computercriminaliteit III

Koops, E.J.

Published in:
Nederlands Juristenblad

Publication date:
2010

Document Version
Peer reviewed version

Tijd voor Computercriminaliteit III

Bert-Jaap Koops[1]

Dit is de uitgebreide versie van het artikel dat is gepubliceerd op de weblocatie van het NJB. Een verkorte versie is gepubliceerd op papier in Nederlands Juristenblad 2010, p. 2461-2466.

Eind juli 2010 publiceerde het Ministerie van Justitie een wetsontwerp "versterking bestrijding computercriminaliteit", dat een ontoegankelijkmakingsbevel voor de officier van justitie regelt, 'heling' van gegevens strafbaar stelt en de strafrechtelijke aansprakelijkheid voor opnemen van communicatie verruimt.[2] De 'snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit roepen voortdurend de vraag op of de juridische instrumenten nog voldoende zijn'.[3] Het is tijd voor een Wet computercriminaliteit III. Maar daarbij moet de wetgever wel de tijd nemen om het wetsvoorstel goed te laten aansluiten op de systematiek van het strafrecht.

1. Achtergrond[4]

Tot 30 september kregen burgers, bedrijven en maatschappelijke organisaties door middel van Internetconsultatie de gelegenheid opmerkingen te maken over het wetsontwerp versterking bestrijding computercriminaliteit.[5] Dit valt toe te juichen: belanghebbenden (en dat is eigenlijk iedereen bij dit onderwerp) kunnen op deze manier commentaar leveren en aldus bijdragen aan betere wetgeving die, als het goed is, aansluit op de behoeften van de maatschappij. Daarbij mogen de systematiek van de wet en fundamentele waarden zoals rechtsbescherming niet uit het oog worden verloren, en daarom is het belangrijk dat ook vanuit de wetenschap kritische reflectie plaatsvindt op het wetsontwerp. In deze bijdrage geef ik een kritische analyse van het wetsontwerp, niet alleen van de voorgestelde bepalingen maar ook van wat er níét in wordt geregeld, waarbij ik met name bekijk hoe het wetsontwerp zich verhoudt tot de systematiek van het strafrecht.

Eigenlijk had ik verwacht dat een nieuw wetsvoorstel ter bestrijding van computercriminaliteit 'computercriminaliteit III' zou heten, in navolging van de Wet computercriminaliteit uit 1993 en de Wet computercriminaliteit II uit 2006.[6] Evenals bij computercriminaliteit II zijn er wel enkele substantiële zaken te regelen, zoals het ontoegankelijkmakingsbevel, maar ook de nodige details te verbeteren, zodat een veelomvattende nieuwe wet – Computercriminaliteit III – op zijn plaats zou zijn. Misschien kiest de wetgever voor een andere naam om niet te suggestie te wekken dat het wetsvoorstel opnieuw een veelomvattende operatie is, maar slechts enkele onderdelen wil regelen. Dat is dan wel een gemiste kans, omdat er toch ook enkele andere onderwerpen zijn die mijns inziens bij dit wetsvoorstel meegenomen zouden moeten worden. Die bespreek ik aan het eind, na een analyse van de voorgestelde maatregelen.[7]

---

[1] Prof.dr. B.J. Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.

[2] Conceptwetsvoorstel versterking bestrijding computercriminaliteit (hierna: wetsontwerp), beschikbaar op http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit (geraadpleegd 11 september 2010).

[3] Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 1 (hierna: MvT).

[4] Een verkorte versie van deze bijdrage is gepubliceerd in de papieren versie van het *Nederlands Juristenblad*, 2010, nr. [xxx].

[5] Zie http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit (geraadpleegd 11 september 2010).

[6] Stb. 1993, 33; Stb. 2006, 399.

[7] Naast de hier behandelde hoofdonderwerpen zorgt het wetsontwerp ook dat de voor computercriminaliteit relevante definities in beide wetboeken worden opgenomen omdat de definities in Sr niet automatisch ook gelden voor Sv (en omgekeerd) (zoals betoogd door F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken*, Nijmegen: WLP 2004, p. 238-240) en verbetert het een foute verwijzing in art. 126bb Sv. Deze laat ik verder buiten beschouwing.

2. Het ontoegankelijk maken van gegevens (NTD)

2.1. Het voorstel

Het belangrijkste – maar ook meest omstreden – onderdeel van het wetsontwerp is de bevoegdheid voor de officier van justitie om een internetaanbieder te bevelen strafbare gegevens ontoegankelijk te maken (zeg maar: van het internet te verwijderen, voor zover in zijn beschikkingsmacht). Daartoe wordt art. 54a Sr aangepast, dat tussenpersonen (internetaanbieders) uitsluit van aansprakelijkheid voor strafbare gegevens indien zij op bevel deze gegevens ontoegankelijk maken, en wordt een nieuwe bevoegdheid voorgesteld voor de officier van justitie ontoegankelijkmaking te bevelen (art. 125p Sv), eventueel onder dwangsom (art. 125q Sv).

Invoering van een zogeheten NTD-bevel (*Notice and Take-Down*) is dringend nodig. Niet dat er nog geen mogelijkheid bestaat om strafbare inhoud van het internet te laten verwijderen: er bestaat een NTD-gedragscode waarbij internetaanbieders vrijwillig inhoud ontoegankelijk maken.[8] Maar vrijwillige medewerking is niet altijd voldoende; wanneer bijvoorbeeld de aanbieder vindt dat het geen evident strafbare gegevens betreft, kan hij medewerking weigeren vanuit het belang van de vrijheid van meningsuiting. Volgens sommigen had de wetgever voor die situaties al een ontoegankelijkmakingsbevel geregeld in art. 54a Sr:[9]

> Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Hierin zou gelezen kunnen worden dat de officier, na rechterlijke machtiging, bevoegd is tot een ontoegankelijkmakingsbevel, maar dat is onaannemelijk: het is onsystematisch (en onwenselijk) een bevoegdheid in het Wetboek van Strafrecht (in plaats van Strafvordering) te regelen, en er ontbreken tal van rechtswaarborgen, zowel voor de geadresseerde als voor de officier. Daarom concludeerde een Cycris-rapport in 2007 dat art. 54a Sr geen grondslag vormt voor een ontoegankelijkmakingsbevel en dat zelfstandige invoering daarvan nodig is.[10] Dat blijkt ook uit een voortslepende zaak in het Noorden, waar een officier twee keer niet-ontvankelijk is verklaard in de vervolging van een internetaanbieder die weigerde te voldoen aan een ontoegankelijkmakingsbevel, omdat de rechter-commissaris daarvoor een machtiging had geweigerd; de r-c had dit gedaan omdat hij art. 54a Sr onvoldoende uitgewerkt vindt voor een bevoegdheidsgrondslag, met name vanwege het ontbreken van rechtsbeschermende waarborgen, zoals een toetsingskader of beroepsmogelijkheden.[11]

Het wetsontwerp regelt daarom een NTD-bevel, wat juist voor gevallen belangrijk is waarin vrijwillige medewerking wordt geweigerd; daarom misschien ook vindt de wetgever dat een dwangsom nuttig kan zijn om het bevel kracht bij te zetten. De vormgeving van het bevel is bepaald verstrekkend:

> De officier van justitie kan van een aanbieder van een communicatiedienst of van degene die de beschikkingsmacht heeft over een geautomatiseerd werk, vorderen om onverwijld alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit nodig is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. (voorgesteld art. 125p lid 1 Sv)

Ontoegankelijkmaking kan dus niet alleen worden gevorderd van internetaanbieders, maar ook van andere communicatieaanbieders; sinds de Wet computercriminaliteit II (zie art. 126la Sv) worden daaronder begrepen niet alleen publieke telecommunicatieaanbieders (die vallen onder de Telecommunicatiewet), maar ook private aanbieders van communicatie: bedrijven en instellingen die voor hun werknemers of een besloten gebruikersgroep bedrijfsmatig email- of

---

[8] Gedragscode Notice-and-Takedown, oktober 2008, http://www.samentegencybercrime.nl/NTD/NTD?p=content (geraadpleegd 11 september 2010).

[9] Ingevoerd bij de Aanpassingswet richtlijn inzake elektronische handel, Stb. 2004, 210.

[10] Schellekens, M.H.M., B.J. Koops & W. Teepe (2007), *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg: TILT/Cycris, augustus 2007.

[11] Rb. Assen 24 november 2009, LJN BK4226, *Mediaforum* (2010), p. 170-172 m.nt. Koops; voorgeschiedenis: Rb. Assen 22 juli 2008, LJN BD8451 en Hof Leeuwarden 20 april 2009, LJN BI1645.

intranetfaciliteiten bieden. Ook zou de vordering gericht kunnen worden aan iedereen die beschikking heeft over een computer. Volgens de toelichting (p. 21) is 'in veel gevallen de medewerking van een derde vereist die de beschikkingsmacht heeft over de gegevens die op het internet zijn geplaatst of in een computer zijn opgeslagen'. Ik kan echter geen situaties verzinnen waarin het nodig zou zijn om een NTD-bevel te geven buiten de context van het internet, wat – ook blijkens de toelichting – de crux is van een *notice-and-take-down*-procedure. Bij losstaande computers kan justitie allicht zelf de computer in beslag nemen of zelf gegevens ontoegankelijk maken (art. 125o Sv). Het gedeelte 'of van degene die de beschikkingsmacht heeft over een geautomatiseerd werk' zou dus kunnen worden geschrapt. Bij aanbieders van besloten netwerken – zoals bedrijfsnetwerken – zal medewerking van derden vaak wel nodig zijn, zeker als het grootschalige netwerken betreft; in die gevallen kan ik mij voorstellen dat een NTD-bevel vergelijkbaar is met de situatie van internetaanbieders.

2.2. De noodzaak van een rechterlijke toets

Veel ingrijpender is echter dat het wetsontwerp geen rechterlijke machtiging vereist voor een ontoegankelijkmakingsbevel. Dat is opmerkelijk, omdat de toetsing door een rechter wel in art. 54a Sr was opgenomen,[12] juist in het licht van de achtergrond van die bepaling van het voorkomen van (zelf)censuur en het grote belang van de vrije meningsuiting bij internet.[13] Het is ook saillant in het licht van het recente Sanoma-arrest, waarin het Europees Hof Nederland op de vingers tikte omdat de wettelijke regeling toelaat dat een officier van justitie een uitleveringsbevel geeft aan journalisten zonder voorafgaande rechterlijke toetsing; dat is in strijd met art. 10 EVRM.[14] Hoewel die zaak journalistieke bronbescherming betreft en niet verwijdering van onrechtmatige publicaties, en daarom geen directe weerslag heeft op een NTD-bevel, zou het wel een teken aan de wand moeten zijn voor de wetgever: inbreuken op de vrije meningsuiting vergen een voorafgaande rechterlijke toets.

Volgens de toelichting is de NTD-bevoegdheid echter goed belegd bij de officier – waarbij men ervan uitgaat dat er 'gespecialiseerde officieren van justitie zijn aangewezen die zijn belast met de beoordeling van de strafbaarheid van de gedragingen op het internet en de wenselijkheid van een vordering op grond van dit artikel te doen' (p. 22) – en is er geen noodzaak voor een rechterlijke toets. Het gaat immers, zegt de toelichting, om een 'maatregel van tijdelijke aard', waarbij beklag kan worden gedaan bij de raadkamer van de rechtbank; of als niet aan de vordering wordt voldaan en op basis van 184 Sr (weigering te voldoen aan een bevel) wordt vervolgd, dan komt de zaak ook voor de rechter. 'Handhaving van voorafgaande machtiging door de rechter-commissaris is daarom niet noodzakelijk' (p. 22).

Om een aantal redenen is deze redenering niet steekhoudend. Ten eerste is de bevoegdheid bedoeld voor moeilijke gevallen. Bij evident onrechtmatige inhoud – zoals prepuberale kinderporno of serieuze bedreigingen van hoogwaardigheidsbeklederS – zal de internetaanbieder vrijwel altijd vrijwillig meewerken.[15] Een NTD-*bevel* is juist van belang in het grijze gebied tussen strafrechtelijke aansprakelijkheid en vrije meningsuiting: puberale kinderpornografie of discriminerende en racistische uitingen waarbij het moeilijk is te bepalen of de uiting nog binnen de grenzen van de vrije meningsuiting valt. Dat vergt een zeer specialistische en casuïstische beoordeling, die in ons rechtsstelsel aan de rechter is toebedeeld. Bij de vrije meningsuiting staat het censuurverbod voorop: een uiting mag worden gedaan *totdat* deze onrechtmatig is beoordeeld, en die beoordeling is aan de rechter. Juist in het grijze gebied moet eerst een rechter oordelen *voordat* gegevens weggehaald kunnen worden. Het huidige voorstel gaat echter uit van eerst weghalen en pas later (mogelijk veel later, zie onder) een rechterlijke toetsing laten uitvoeren. Dat is de omgekeerde wereld.

Ten tweede is het maar de vraag of er uiteindelijk wel een rechter aan te pas zal komen. Volgens de toelichting gebeurt dat na verloop van tijd – het is immers een tijdelijke maatregel – wanneer a) een belanghebbende beklag doet bij de rechtbank of b) het OM vervolgt na weigering. In geval a), als de aanbieder de gegevens weghaalt, zal hijzelf of de oorspronkelijke inhoudsaanbieder

[12] Zie boven, par. 2.1.

[13] Zie daarvoor de Richtlijn elektronische handel, 2000/31/EG en de toelichting bij de implementatiewet, Kamerstukken 28 197.

[14] EHRM 14 september 2010, Appl.No. 38224/03 (Sanoma Uitgevers t. Nederland).

[15] Vgl. 'In die gevallen *waarin de NTD-gedragscode niet afdoende is* voor de verwijdering van de gegevens, kan de officier van justitie gebruik maken van de bevoegdheid van het voorgestelde artikel 125p Sv' (p. 4, mijn cursivering).

beklag moeten doen als zij vinden dat de inhoud niet strafbaar is; een internetaanbieder zal dat zelf niet snel doen (zij hebben immers meestal 'geen boodschap aan de boodschap'), een enkele activistische Internetaanbieder uitgezonderd. Voor de inhoudsaanbieder is de stap naar de rechter misschien een grote stap, zeker als hij in het buitenland woont en geen idee heeft hoe het Nederlandse rechtssysteem werkt.
Daarbij komt dat er geen regeling wordt getroffen dat de inhoudsaanbieder zelf wordt ingelicht over het verwijderen van diens gegevens. Als ik het goed zie, bestaat er geen notificatieplicht – noch de notificatieregeling van art. 125m Sv (bij vastlegging van gegevens bij een doorzoeking) noch die van art. 126bb Sv (bij bijzondere opsporingsbevoegdheden) is van toepassing. (Nog daargelaten of notificatie door justitie aan betrokken inhoudsaanbieders in de praktijk zou plaatsvinden, gezien de ervaringen bij de BOB-notificatie,[16] zeker als niet direct de naam-adres-woonplaats-gegevens van inhoudsaanbieders bekend zijn.) Evenmin wordt de internetaanbieder verplicht om zijn klant in te lichten. Het komt er dus op neer dat degene die ergens een omstreden uiting blogt of twittert er zelf maar moet achterkomen dat de uiting is verwijderd, en dan zelf zal moeten bedenken dat hij naar de raadkamer van de rechtbank kan stappen om zijn recht ex art. 552a Sv (beklag) uit te oefenen.
In geval b), als de aanbieder weigert aan het bevel te voldoen, is het ook nog maar de vraag of het OM de aanbieder gaat vervolgen wegens het niet voldoen aan een ambtelijk bevel. Vervolgingen van bedrijven op basis van art. 184 Sr komen zelden voor (denk ik, ik heb het niet uitgezocht). Dat is niet verwonderlijk, omdat er nogal een stap zit tussen het doen van een bevel en het vervolgen voor niet-nakoming. Het laatste vergt meer inspanning, tijd en middelen, en brengt bovendien een risico mee van imagoschade wanneer de rechter zou oordelen dat de gewraakte inhoud toch niet strafbaar zou zijn (nogmaals, het gaat vaak om moeilijke gevallen). Het huidige voorstel bergt een groot risico in zich dat het OM de bevoegdheid te makkelijk gaat inzetten: nee heb je, ja kun je krijgen. De officier zou in twijfelgevallen wel een bevel kunnen geven tot ontoegankelijkmaking maar vervolgens eieren voor zijn geld kunnen kiezen als de aanbieder weigert.[17] Juist daarom kan een rechterlijke toets niet worden gemist.
Er zijn nog twee mogelijkheden waarbij de (vermeend) strafbare inhoud ter toetsing aan de rechter wordt voorgelegd. Wanneer de inhoudsaanbieder (of de internetaanbieder, als deze voldoende bij de inhoud betrokken is om medeplichtig te zijn) wordt vervolgd, zal de rechter zich ook uitspreken over de strafbaarheid van de gegevens, maar ook dat hangt af van de vervolgingsbereidheid van het OM (met alle capaciteitsgebrek en prioriteiten in de opsporing van dien). Daarnaast kan de officier ook zelfstandig vorderen bij de rechter om bij afzonderlijke beschikking ontoegankelijk gemaakte gegevens te vernietigen (een eindbeslissing over 'onttrekking aan het verkeer' van gegevens voor het geval de inhoudsaanbieder niet zelf wordt vervolgd) conform art. 552fa Sv, dat hiertoe in het wetsontwerp wordt aangepast. Maar dit is een bevoegdheid en geen verplichting van het OM, en eerlijk gezegd kan ik me nauwelijks voorstellen dat het OM, als een aanbieder gegevens op het internet ontoegankelijk heeft gemaakt, nog de moeite zou nemen om vervolgens definitieve vernietiging van deze gegevens te vorderen.
Het lijkt mij al met al sterk de vraag of een bevel tot ontoegankelijkmaking van gegevens in de praktijk uiteindelijk door een rechter getoetst zal worden. Daarvoor zitten er te veel gaten en onzekerheden in de regeling. Dat betekent dat in veel gevallen de 'tijdelijke maatregel' vanzelf een definitieve maatregel wordt, zonder dat een rechter ernaar gekeken heeft.
Zou er nog een bepaalde reden kunnen zijn om af te zien van een rechterlijke toets vooraf? Een van de manco's van de huidige (non-)regeling in art. 54a Sv is het gebrek aan rechtsmiddelen, waaronder een beroepsmogelijkheid voor de officier indien de r-c een machtiging weigert (daar had ook de officier in de Assense zaak[18] last van). Dat is echter geen probleem bij de huidige regeling: nu een ontoegankelijkmakingsbevel in het Wetboek van Strafvordering wordt geregeld, staat automatisch een beroep van de officier bij de rechtbank open tegen beschikkingen van de rechter-commissaris (art. 446 Sv). Een andere mogelijke reden (die niet wordt genoemd in de toelichting maar onderhuids zou kunnen meespelen) is dat een rechterlijke machtiging tijd kost en dat het om urgente zaken gaat. Dat argument snijdt evenmin hout. Tegenwoordig bestaan er

[16] A. Beijer et al., *De Wet bijzondere opsporingsbevoegdheden – eindevaluatie*, Meppel: WODC/Boom juridische uitgevers 2004, p. 145-147.
[17] Men zou om dit te voorkomen een verplichting kunnen invoeren voor de officier om te gaan vervolgen na weigering te voldoen aan het bevel, maar dat strookt niet met het opportuniteitsbeginsel.
[18] *Supra*, noot 11.

immers mobiele telefoons, zodat r-c's in principe direct bereikbaar zijn en telefonische machtigingen (later schriftelijk te bevestigen) kunnen geven. Dat was bij de Wet herziening van het gerechtelijk vooronderzoek juist het argument om een rechterlijke toets te hanteren niet alleen bij de reguliere doorzoeking maar ook bij een spoeddoorzoeking.[19]
Ik concludeer dat er geen steekhoudende argumenten zijn tegen een voorafgaande rechterlijke toets bij een ontoegankelijkmakingsbevel. Het zal vaak gaan om moeilijke gevallen waarbij de inhoud niet evident strafbaar is, en het zal in veel gevallen ook niet een tijdige maar een definitieve maatregel betreffen. Het belang van de vrije meningsuiting, en het censuurverbod van art. 7 Gw en 10 EVRM, eisen dat de rechter zich uitlaat voordat justitie verwijdering van gegevens kan bevelen.

2.3. De dwangsom

Het voorstel om ontoegankelijkmaking onder dwangsom te kunnen bevelen, is al even opmerkelijk als het weglaten van rechterlijke toetsing. Artikel 125q Sv stelt dat de officier in de vordering een dwangsom kan opleggen, dat wil zeggen een verplichting tot betaling van een geldsom – een totaalbedrag of een bedrag per tijdseenheid tot een bepaald maximum – indien niet of niet tijdig aan de vordering wordt voldaan. Het opleggen van de dwangsom wordt daarbij gereguleerd door diverse bepalingen uit de Algemene wet bestuursrecht.[20] Een dergelijke mogelijkheid bestaat nog niet in het strafrecht. Op basis van een aanbeveling in het WODC-rapport *De WED op de helling* (2005) geeft de wetgever nu echter de voorkeur aan een last onder dwangsom boven een vervolging voor het niet voldoen aan een ambtelijk bevel, omdat dit effectiever en doelmatiger is bij spoedeisende maatregelen.[21] Dat mag dan zo zijn, maar het is nogal een systeembreuk met de systematiek van strafvordering om dit bestuursrechtelijke element op te nemen in het Wetboek van Strafvordering. De onderbouwing daarvan is bepaald mager, zeker omdat de toelichting stelt dat gezien de bereidwilligheid van internetaanbieders om vrijwillig inhoud te blokkeren, opleggen van een dwangsom in de praktijk niet vaak nodig zal zijn.[22] Juist bij een ingrijpende systematische verandering van het strafrecht mag men toch een substantiële empirische onderbouwing verwachten waarom een nieuw type bevoegdheid niet kan worden gemist in het strafvorderlijke stelsel. Ik kan in het kader van de strafvordering wel de nodige andere bevelen bedenken (zoals een bevel tot uitlevering of tot verstrekking van bepaalde gegevens) waar in de praktijk meer behoefte bestaat aan een stevige stok achter de deur om de geadresseerde aan te zetten tot medewerking, dan bij een NTD-bevel nodig zal zijn. De wetgever zou er beter aan doen de dwangsom niet via dit wetsvoorstel in het strafrecht binnen te smokkelen, maar – als hij het echt nodig vindt – een apart wetsvoorstel te concipiëren dat een integrale visie en vooral ook een gedegen onderbouwing geeft voor de situaties waarin een dwangsom zou moeten kunnen worden opgelegd bij spoedeisende maatregelen binnen de strafvordering.

2.4 Overige aspecten

Het feit dat een dwangsom wordt voorgesteld roept de vraag op of het hier eigenlijk wel om strafvordering gaat, of meer om bestuurs(straf)recht of pseudo-strafrecht. Systematisch past een ontoegankelijkmakingsbevel – met als hoofddoel om gegevens van het internet te halen – niet goed in de klassieke strafvordering die gericht is op bewijsvergaring, vervolging en berechting. De ontoegankelijkmaking kan immers losstaan van een strafvorderlijk traject om de inhoudsaanbieder te vervolgen; zeker als deze in het buitenland zit, zal vervolging al snel achterwege blijven. De ontoegankelijkmaking is er vooral op gericht om strafbare gegevens te onttrekken aan het verkeer, maar zonder dat dit per se in het kader van een strafrechtelijke vervolging plaatsvindt (al zal dat in voorkomende gevallen, mag men hopen, wel gebeuren). Dat heeft consequenties voor de omgang met de gewraakte gegevens: stel dat de internetaanbieder de gegevens ontoegankelijk maakt, wat gebeurt er dan verder met deze gegevens?
Wanneer de inhoudsaanbieder wordt vervolgd, zal de rechter ter zitting ook een uitspraak moeten doen over de ontoegankelijk gemaakte gegevens (voorgestelde aanpassing van art. 354 lid 1

[19] *Kamerstukken II* 1994/95, 23 251, nr. 9, p,. 8.
[20] Artt. 4:97, 4:112, 4:114, 4:115, 4:116, 4:120 tot en met 4:124, 5:33 en 5:34 Awb worden van overeenkomstige toepassing verklaard (voorgesteld art. 125q lid 5 Sv).
[21] MvT, p. 25.
[22] MvT, p. 26.

Sv). Het wetsontwerp vergeet hierbij om art. 354 lid 2 Sv aan te passen; dat bepaalt nu dat de rechtbank besluit dat de gegevens (als ze strafbaar zijn) worden vernietigd of (als ze niet strafbaar zijn) weer ter beschikking worden gesteld 'van de beheerder van het geautomatiseerd werk'. In het eerste geval – vernietiging – moet dan niet specifiek worden bepaald dat de officier een nieuwe vordering doet aan de aanbieder om de gegevens nu te vernietigen? De last van de rechtbank lijkt mij in de huidige vorm gericht aan het Openbaar Ministerie, niet aan een derde. In het tweede geval – teruggave – gaat het om gegevens terug te geven die ontoegankelijk zijn gemaakt door justitie zelf in het kader van een doorzoeking (art. 125o Sv). Wanneer de internetaanbieder ex 125p Sv gegevens ontoegankelijk heeft gemaakt, zal hij ze – als beheerder van de server – nog in zijn beschikking hebben, dus lid 2 is dan een loze bepaling. De wet zou moeten specificeren wat de internetaanbieder in dit geval moet doen: de gegevens teruggeven aan de inhoudsaanbieder, of de gegevens weer toegankelijk maken op internet, of mag hij zelf maar zien wat hij doet?
Wat ook lijkt te ontbreken is een verplichting voor de internetaanbieder om de gegevens wel zelf vast te houden totdat er een definitief oordeel door de rechter is geveld; art. 354 Sv veronderstelt in die zin een bewaarplicht voor de internetaanbieder, voor het geval het uiteindelijk toch niet om strafbare gegevens blijkt te gaan. Moet dat dan niet in het bevel worden vermeld? Maar een lastig punt daarbij is dat, zoals ik hierboven betoogde, het lang niet altijd tot een einduitspraak hoeft te komen, en dan kan de internetaanbieder de ontoegankelijk gemaakte gegevens tot sint-juttemis bewaren. Het ligt meer voor de hand dat de aanbieder ten tijde van de ontoegankelijkmaking een kopie van de gegevens aan justitie geeft, waarbij justitie de verplichting heeft deze te bewaren tot een definitieve einduitspraak. Mutatis mutandis gelden deze opmerkingen ook voor art. 552fa Sv (waarbij de rechter bij afzonderlijke beschikking een definitief besluit neemt over de gegevens).
Tot slot wijs ik nog op een wetssystematisch probleem. De voorgestelde bevoegdheid komt terecht in een afdeling (Eerste boek, Titel IV, zevende afdeling) waar het nauwelijks iets mee te maken heeft: de doorzoeking ter vastlegging van gegevens. Er vindt geen doorzoeking plaats, de gegevens staan immers op internet. Ik weet niet waar de bevoegdheid dan wel zou thuishoren; het past evenmin bij de bijzondere opsporingsbevoegdheden, het gaat immers niet bepaald om opsporing. Wellicht is een beter aanknopingspunt titel VIA van het Vierde Boek, 'Strafvordering buiten het gebied van de rechtbank'? In sommige opzichten is de internetaanbieder vergelijkbaar met de schipper die bepaalde verplichtingen heeft in het kader van de strafvordering. In elk geval zou nog eens goed gekeken kunnen worden naar de plaatsing in het Wetboek, die onder andere van belang is in verband met het karakter van de maatregel in het licht van de afdeling waarin deze is ondergebracht, en de procedures en rechtswaarborgen die voor zo'n afdeling in het bijzonder gelden.

3. 'Heling' en 'verduistering' van computergegevens

Artikel 139e Sr stelt momenteel het bezit en verspreiden van wederrechtelijk afgetapte gegevens strafbaar. Het wetsontwerp breidt deze bepaling vergaand uit tot bezit of verspreiding van alle vormen van wederrechtelijk verkregen gegevens, kortweg aan te duiden als 'heling' van gegevens. De reden daarvan is dat door de voortschrijdende technische ontwikkelingen gegevens beter beschermd moeten worden door het strafrecht. Steeds meer komt het immers voor dat gegevens op internet terecht komen en dan razendsnel voor grote groepen toegankelijk zijn, terwijl het – zoals de toelichting (p. 6) met de nodige onderdrijving schrijft – 'bovendien niet eenvoudig [is] om over het internet verspreide gegevens daarvan geheel verwijderd te krijgen'. Publicatie van gehackte gegevens valt niet te vervolgen via de huidige helingbepaling, omdat gegevens geen 'goed' zijn, noch kan een derde-verkrijger worden vervolgd voor computervredebreuk. Ook valt, wanneer gegevens bij iemand worden aangetroffen, niet altijd te bewijzen dat hijzelf deze wederrechtelijk heeft verkregen. Om die redenen wordt 'heling' van computergegevens strafbaar gesteld, met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (voorgesteld art. 139e Sr), vergelijkbaar met schuldheling van goederen (art. 417bis Sr).
Voorts breidt het wetsontwerp art. 139c Sr uit door het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens uit een computer strafbaar te stellen. Volgens de toelichting is dit vooral van belang voor gevallen waarin de dader wel rechtmatig toegang heeft tot gegevens (en dus niet computervredebreuk pleegt) maar geen titel heeft de gegevens over te nemen voor zichzelf of een ander, bijvoorbeeld een werknemer die gegevens (adressenbestanden of

bedrijfsgeheimen) overneemt om voor zichzelf te gebruiken. Dit komt min of meer neer op 'verduistering' van gegevens'.[23]
Beide voorstellen versterken de systematiek van het strafrecht, voor zover ze – in lijn met de Wet computercriminaliteit – bepalingen invoeren voor gegevens die analoog zijn aan bepalingen voor goederen (huisvredebreuk-computervredebreuk; zaakbeschadiging-gegevensbeschadiging; enz.). Heling en verduistering van gegevens waren nog niet strafbaar, en er valt veel voor te zeggen dat te doen, gezien het grote belang van computergegevens voor de samenleving maar ook voor de persoonlijke levenssfeer en het gemak waarmee gegevens tegenwoordig verspreid raken buiten de controle van rechthebbenden. De Wet bescherming persoonsgegevens kan daar in de praktijk niet altijd veel aan verhelpen, en dan kan het raadzaam zijn om ook een vangnet van strafrechtelijke aansprakelijkheid te hebben.
Deze strafrechtelijke aansprakelijkheid gaat wel ver bij de 'verduistering' van gegevens. Soms zijn er redenen zijn om gegevens wederrechtelijk (bijvoorbeeld in strijd met een arbeidscontract) over te nemen en te publiceren, met name in het geval van klokkenluiders. Op hen zou de strafbaarstelling een zelfcensurerend effect kunnen hebben.[24] Dat is een valide argument, dat misschien ondervangen kan worden door een duidelijke toelichting van de wetgever dat klokkenluiden een rechtvaardigingsgrond is.
Maar ook voor het algemene publiek is de strafbaarstelling vergaand. In een kenniseconomie waarin een groot deel van de werknemers met computers werkt, waarbij die computers in veel gevallen mobiel zijn of via telewerken toegankelijk zijn, en de werknemers regelmatig thuiswerken, worden er enorm veel niet-openbare gegevens 'overgenomen voor zichzelf'. Cruciaal wordt dan de beoordeling wanneer deze overname wederrechtelijk is of wordt. Op welk moment wordt duidelijk dat de werknemer het adressenbestand (dat hij altijd op een usb-staafje meeneemt voor zijn thuiswerkdag) niet voor zijn werkgever gebruikt maar voor zichzelf (en wat betekent dat dan precies)? Wanneer een echtgenoot de mail van zijn man op hun gezamenlijke computer leest en een bericht kopieert met het vage idee dat hij dat later misschien kan gebruiken bij een echtscheidingsprocedure om geen alimentatie te hoeven betalen, is die overname dan wederrechtelijk, en zo ja, is dat op het moment van kopiëren, op het moment dat hij daadwerkelijk besluit te scheiden, of op het moment dat hij het gekopieerde bericht in de strijd gooit? Hier zou de wetgever de wetsbepaling, of tenminste de Memorie van Toelichting, mogen uitbreiden met een omschrijving van wat precies strafwaardig gedrag is aan het overnemen van niet-openbare gegevens.
Bij 'heling' van gegevens is de strafrechtelijke aansprakelijkheid ook ruim, maar iets minder gevaarlijk voor de gemiddelde computergebruiker omdat er een redelijk vermoeden moet bestaan dat de gegevens uit misdrijf zijn verkregen. Wetssystematisch vallen wel drie kanttekeningen te plaatsen bij de voorgestelde bepaling in art. 139e lid 1 Sr. Ten eerste wordt 'heling' beperkt tot gegevens die wederrechtelijk zijn verkregen door afluisteren, aftappen, opnemen of overnemen van telecommunicatie of computergegevens, wat erop neerkomt dat de gegevens door computercriminaliteit zijn verkregen. Dat wijkt af van de helingbepalingen (art. 416, 417bis Sr) die geen onderscheid maken naar het misdrijf. Het valt moeilijk in te zien waarom heling van computergegevens strafwaardig is wanneer de gegevens oorspronkelijk zijn gehackt of afgeluisterd, maar niet wanneer de gegevens zijn verkregen door diefstal van een laptop, afpersing, oplichting of welk ander misdrijf dan ook waarmee je gegevens kunt vergaren. Zal een derde-verkrijger die geacht wordt de misdadige afkomst van gegevens te kennen of vermoeden kunnen onderscheiden of de gegevens zijn gehackt of gestolen? Dat lijkt mij moeilijk vol te houden. Ten tweede wijkt de voorgestelde bepaling af van de helingbepalingen door niet te spreken van het 'verwerven' of 'voorhanden krijgen' (zoals art. 416 en 417bis) maar van 'beschikking hebben', wat een passievere handeling is dan verwerven of voorhanden krijgen. Dat wordt misschien gecompenseerd door het kennisvereiste (wat bewustzijn van de dader vergt), maar niet helemaal: als iemand in de krant leest dat de naaktfoto van een bekende Nederlander uit haar computer is ontvreemd en op internet is gepubliceerd, en vervolgens nieuwsgierig die webpagina bekijkt, zal de foto in zijn cache komen te staan en heeft hij dus beschikking over gegevens waarvan hij weet dat die gehackt waren, maar zonder dat hij zich bewust hoeft te zijn

[23] MvT, p. 9.
[24] Zoals betoogd door in een brief van 15 september 2010 van organisaties, wetenschappers en bloggers, geïnitieerd door Bits of Freedom, https://www.bof.nl/2010/09/15/persbericht-nederlandse-internetgemeenschap-protesteert-tegen-overheidscensuur/ (geraadpleegd 18 september 2010).

dat hij zelf nu ook over die gegevens beschikt. Daarom zou een formulering als 'beschikking verwerft' beter passen om 'heling' strafbaar te stellen. Ten derde ontbreekt ook de clausule 'ten tijde van de verwerving of het voorhanden krijgen' die bij heling geldt voor het kennisvereiste: je bent alleen een heler als je op het moment van verwerving de onrechtmatige afkomst kent of moest vermoeden. Die clausule ontbreekt in voorgesteld art. 139e Sr, zodat ook als de computereigenaar pas achteraf kennis krijgt (of zou moeten krijgen) van de strafrechtelijke afkomst hij schuldig wordt aan gegevensheling. Je mag dan de krant en nieuwsblogs wel goed bijhouden of die gedownloade pikante Flickr-foto's niet plotseling gehackt blijken uit de computer van je favoriete filmster. Deze verschillen met de helingbepaling worden niet gemotiveerd in de toelichting.
Tot slot nog een kanttekening: in art. 139e onder b Sr wordt ook het opzettelijk ter beschikking stellen aan een ander van gehackte (enz.) gegevens strafbaar. Volgens mij ontbreekt daarbij een wederrechtelijkheidseis; het zou toch immers niet strafbaar moeten zijn voor een derde om door misdrijf verkregen gegevens ter beschikking te stellen van de politie of van het slachtoffer om hen in kennis te stellen van de rondslingerende gegevens? Bovendien zou een wederrechtelijkheidseis ook het bezwaar ondervangen dat journalisten soms uit misdrijf verkregen – bijvoorbeeld afgetapte – gegevens moeten kunnen publiceren, in het publiek belang.[25] De Memorie van Toelichting zou dan kunnen expliciteren dat in zwaarwegende (journalistieke) gevallen de publicatie van de gegevens niet onrechtmatig is.

4. Het opnemen van gesprekken door gespreksdeelnemers

Bij de strafbaarstelling van wederrechtelijk aftappen of opnemen van communicatie (art. 139a-c Sr) geldt tot nu toe een uitzondering voor afluisteren of opnemen door gespreksdeelnemers zelf. Dat is een bewuste keuze van de wetgever geweest: wie gesprekken aangaat, neemt het risico dat de ander het gesprek opneemt en daar dan mogelijk iets mee doet.[26] Maar nu de techniek het heimelijk opnemen makkelijker maakt dan ooit, en bovendien wereldwijde verspreiding van de opname slechts een paar muisklikken vergt, wordt het risico van ongewenste verspreiding van privégesprekken wel erg groot. Daarom stelt het wetsontwerp in art. 139a (gesprekken in besloten ruimten), 139b (gesprekken in niet-besloten ruimten) en 139c Sr (telecommunicatie en computergegevensuitwisseling) ook het wederrechtelijk opnemen door gespreksdeelnemers zelf strafbaar. In uitzonderingsgevallen – bijvoorbeeld wanneer een journalist een gesprek zonder toestemming van de gesprekspartner opneemt om misstanden aan de kaak te stellen – zal het opnemen niet wederrechtelijk worden geacht.[27]
Het strafbaarstellen van opnemen van gesprekken door gespreksdeelnemers is vooral een rechtspolitieke keuze; destijds vond onze wetgever het niet nodig, maar de Duitse en Franse wetgever wel.[28] Het argument dat de afluistertechniek en vooral de verspreidbaarheid van gegevens nogal zijn veranderd sinds de strafbaarstelling in 1971 is zeker valide; de kans dat je gesprekspartner dat vertrouwelijke gesprek opneemt is misschien niet eens zo veel groter dan destijds (hoewel de apparatuur wel veel kleiner en goedkoper is geworden), maar de kans dat het gesprek vervolgens bij een breed publiek bekend wordt, en daarmee schade aanricht, is wel vele malen groter geworden, en daarmee is het risico (kans vermenigvuldigd met schade) aanzienlijk vergroot. De beleidswijziging valt in dat licht zeker te billijken.
Op één punt kan ik het wetsontwerp echter niet goed volgen. Bij het wederrechtelijk opnemen van gesprekken in een niet-besloten ruimte (art. 139b Sr) wordt als eis gesteld dat het opnemen heimelijk gebeurt, dus niet zichtbaar of kenbaar voor de gesprekspartner; voor de opname van gesprekken binnen besloten ruimten (art. 139a Sr) geldt geen eis van heimelijkheid, behalve als het opnemen met zichtbare apparatuur 'kennelijk misbruik' betekent (lid 2 onder 2). Dat komt erop neer dat het wederrechtelijk opnemen van een eigen gesprek *wel* strafbaar is binnen een woning als je dat doet met zichtbare apparatuur maar daarvan kennelijk misbruik maakt (wat dat dan ook precies betekent) maar niet als je dat doet met zichtbare apparatuur op straat (los van of je die apparatuur 'misbruikt'). Ik snap het verschil niet goed, en vraag me af of het element 'wederrechtelijk' niet gewoon kan volstaan (met weglating van eisen van heimelijkheid of kennelijk misbruik) om aan te geven dat je een gesprek in casu niet zou mogen opnemen.

[25] Ibid.
[26] *Kamerstukken II* 1967/68, 9419, nr. 3, p. 5.
[27] MvT, p. 12.
[28] De MvT verwijst daarbij naar art. 201 Strafgesetzbuch en art. 226-1 en 226-2 Code Pénal.

5. Suggesties voor nog te regelen onderdelen

Aangezien het wetsontwerp naast bovenstaande onderdelen ook twee details regelt (definities en een technische correctie),[29] wekt het toch een beetje de indruk een wetsvoorstel computercriminaliteit III te zijn, waarbij bestaande onvolkomenheden in de computercriminaliteitswetgeving worden aangepakt. Wanneer ik de wetgeving zoals die sinds Computercriminaliteit II luidt bestudeer, vallen mij diverse (mogelijke) inconsistenties en omissies op. Ik noem ze hier kort, in redelijk willekeurige volgorde, in de hoop dat de wetgever deze alsnog meeneemt in het uiteindelijke wetsvoorstel. Deze suggesties kunnen misschien ook bijdragen aan de bestrijding van computercriminaliteit, maar in elk geval versterken ze de wetssystematiek.
In het Wetboek van Strafrecht is, ter implementatie van art. 6 Cybercrime-Verdrag, misbruik van hulpmiddelen strafbaar gesteld in art. 139d lid 2 en art. 161sexies lid 2. Deze artikelen zien op voorbereiding van alle relevante computermisdrijven, behalve virusverspreiding (art. 350a lid 3 Sr). De toelichting gaf aan dat virusverspreiding zelf al een voorbereidingshandeling betreft,[30] maar dat is beperkt tot het verspreiden of beschikbaarstellen van virussen, en ziet niet op verkoop, vervaardigen of andere voorbereidingshandelingen die onder art. 139d lid 2 vallen. Volgens mij is hier het Cybercrime-Verdrag onvoldoende (althans onsystematisch) geïmplementeerd.
Een andere, en mijns inziens de grootste, omissie is dat bij onderzoek van computers de bevoegdheid om ontsleuteling of ongedaanmaking van beveiliging te vorderen (art. 125k Sv) sinds de Wet computercriminaliteit II niet meer kan worden gegeven bij elke vorm van doorzoeking, maar alleen in het kader van een doorzoeking ter vastlegging van gegevens (art. 125i Sv) en een netwerkzoeking (art. 125j Sv). Bij een traditionele doorzoeking ter inbeslagneming – waar evengoed computers en gegevensdragers zullen worden aangetroffen, die niet zelden in beslag worden genomen – kan de bevoegdheid niet worden toegepast. Het is de vraag of de wetgever dat bedoeld of voorzien heeft, maar de wettekst laat moeilijk een andere lezing toe. Volgens mij zou art. 125k Sv moeten gelden voor elke beveiligde computer of versleutelde gegevens die in het kader van de strafvordering worden onderzocht.[31]
Voorts bestaat er een verschil in de rechtswaarborgen tussen onderzoek van een geautomatiseerd werk en het vorderen van gegevens, ofschoon dat in feite communicerende vaten zijn. Terwijl de notificatieplicht vergelijkbaar is geregeld (zie art. 125n en 126bb Sv), verschilt de vernietigingsplicht: BOB-gegevens – inclusief gegevens die gevorderd zijn van een houder – moeten namelijk bewaard worden tot twee maanden na afloop van de zaak (art. 126cc Sv), terwijl door de politie zelf vastgelegde gegevens volgens artikel 125n vernietigd moeten worden zodra ze niet meer van belang zijn.
Ook lijkt het mij onsystematisch dat de vernietigingsplicht (art. 125n) zich beperkt tot gegevens die zijn vastgelegd bij een doorzoeking, en dus niet ziet op gegevens die zijn overgenomen uit bijvoorbeeld een inbeslaggenomen computer. En waarom verwijst de doorzoeking ter vastlegging van gegevens in artikel 125i naar artikel 98 Sv ('brieven en andere geschriften') en niet naar het speciaal op gegevens toegesneden artikel 125l Sv?
Bij de Wet computercriminaliteit II heeft de wetgever het aftappen (art. 126m Sv) verruimd van openbare telecommunicatie tot het aftappen van communicatie via aanbieders van communicatiediensten, waaronder ook private netwerken vallen. Bij een privaat netwerk hoeft de aanbieder niet per se mee te werken (hij valt niet onder de Telecommunicatiewet); in dat geval mag justitie zelf zijn netwerk gaan tappen. Een probleem bij aftappen door justitie zelf is echter dat artikel 126m niets zegt over het betreden van besloten plaatsen zonder toestemming van de rechthebbende, ter uitvoering van het bevel, iets wat artikel 126l Sv (direct afluisteren) wel doet. Dit suggereert – bevoegdheden moeten immers duidelijk worden vastgelegd, en de wetgever vond het bij direct afluisteren nodig om het betreden expliciet te regelen – dat de opsporingsambtenaar niet op basis van artikel 126m het pand van de communicatieaanbieder

[29] *Supra*, noot 7.
[30] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 36.
[31] Daarnaast kan men zich afvragen waarom een ontsleutelbevel bij gevorderde gegevens (126nh/uh/zp Sv) alleen 'bij of terstond na' de vordering kan worden gegeven, terwijl zo'n tijdsbeperking ontbreekt bij het ontsleutelbevel bij onderzoek van een geautomatiseerd werk (125k Sv). Evenzo is mij onduidelijk waarom beklag (art. 552a Sv) wel mogelijk is bij een ontsleutelbevel (dus 125k lid 2 Sv) maar niet bij de vergelijkbare vordering om beveiliging van een computer ongedaan te maken (125k lid 1); ik zie geen reden voor dit onderscheid in rechtsbescherming.

mag betreden (althans niet zonder diens toestemming) om het aftappen voor te bereiden of uit te voeren. Het is daarom de vraag of het zelf aftappen door justitie überhaupt mogelijk is op basis van artikel 126m Sv, en of de officier niet zijn veelal zijn toevlucht zal moeten nemen tot artikel 126l Sv.
Soms zal het voor een beheerder van een bedrijfsnetwerk aantrekkelijker zijn zelf te tappen, bijvoorbeeld als het gaat om de netpost van één werknemer, dan om justitie toe te laten op het hele netwerk; hij wordt daartoe in de gelegenheid gesteld (art. 126m lid 4 Sv), maar zijn medewerking is vrijwillig. De kosten die de aanbieder hierbij maakt, komen echter niet in aanmerking voor vergoeding: artikel 592 Sv vergoedt alleen kosten bij gegevensvordering en ontsleutelbevel, en de Wet tarieven in strafzaken biedt alleen een grondslag voor vergoeding bij *verplichte* medewerking. Zouden niet ook de kosten voor vrijwillige medewerking aan het tappen moeten kunnen worden vergoed?
Het invoeren bij Computercriminaliteit II van het begrip 'aanbieder van een communicatiedienst' (art. 126la Sv) heeft het Wetboek er niet duidelijker op gemaakt. Op diverse plaatsen hanteert de wetgever nog het 'oude' begrip van een openbaar telecommunicatienetwerk (zie vooral art. 138a lid 3 en 350a lid 2 Sr en 125la, 126i, 126ii Sv); het is niet altijd duidelijk waarom deze bepalingen alleen openbare telecommunicatie en niet ook (grote) besloten bedrijfsnetwerken betreffen, terwijl de wetgever deze wel op één lijn heeft gesteld bij andere bepalingen (zoals in art. 273d Sr en 126m Sv).

6. Afsluiting

Het is verheugend dat de wetgever tijd heeft uitgetrokken voor een openbare consultatie van het wetsontwerp. Het zou misschien nog mooier zijn als dit was gebeurd, zoals in Engeland wel gebruikelijk is, in de vorm van een notitie met discussiepunten, waarbij niet alleen voorstellen worden voorgelegd maar ook vragen worden gesteld en meningen over verschillende opties worden geïnventariseerd. Dan zouden ook hete hangijzers aan de orde kunnen zijn gesteld, zoals de vraag of identiteitsdiefstal/fraude zelfstandig strafbaar moet worden gesteld en de vraag of en zo ja wanneer computergegevens toch als 'goed' kunnen gelden (zoals bij 'goederen' in virtuele werelden die geld waard zijn). Dat zijn vragen waarover de literatuur verdeeld of nog niet uitgekristalliseerd is[32] maar waarbij de wetgever eigenlijk wel binnen afzienbare tijd – ten behoeve van de rechtszekerheid – een keuze zou moeten maken. Een open consultatie zou daarbij kunnen helpen.
Wat daar ook van zij, in elk geval helpt dit wetsontwerp ons een stap verder. Hoewel makkelijk gezegd wordt dat de wetgever bij computercriminaliteit altijd achterloopt door de 'snelle technische ontwikkelingen', valt het met dat achterlopen nogal mee. Voor het overgrote deel is de wetgeving rond computercriminaliteit in Nederland prima op orde;[33] het komt eigenlijk vooral aan op de uitvoering van de wetgeving (en de daarvoor benodigde middelen, expertise en prioriteiten). Dat wil niet zeggen dat er niets te verbeteren valt, en ook daarom valt het toe te juichen dat de wetgever met dit wetsontwerp probeert om de wetgeving nog beter bij de tijd te brengen.
Maar dan mogen we wel verwachten dat het om zorgvuldige wetgeving gaat, die nieuwe regelingen invoert die passen in het systeem van de wet. In diverse opzichten schiet het wetsontwerp daarin tekort. Bij een ontoegankelijkmakingsbevel kan een rechterlijke toets vooraf niet worden gemist, en de noodzaak om een dwangsom in het Wetboek van Strafvordering in te voeren is, zacht uitgedrukt, slecht onderbouwd. De strafbaarstelling van 'heling' van computergegevens zou beter aan moeten sluiten bij de formulering van de bestaande helingbepalingen. Daarnaast vallen sommige details van de voorstellen nog te verbeteren of in elk geval nader te onderbouwen. En als er dan toch verbeterd wordt, dan zijn er nog diverse

[32] Vgl. U.R.M.Th. de Vries e.a. (2007), *Identiteitsfraude: een afbakening*, Utrecht, juli 2007, p. 254; N. van der Meulen (te verschijnen), *Fertile Grounds: the Facilitation of Financial Identity Theft in the United States and the Netherlands*; J. Hoekman en C. Dirkzwager (2009), 'Virtuele diefstal: hoe gegevens toch weer goederen werden', *Computerrecht*, p. 158-161; Y. Moszkowicz (2009), 'Een kritische noot bij de 'RuneScape'- en 'Habbohotel'-uitspraken: een illusie is geen goed', *Strafblad*, p. 495-503.
[33] Zoals ik concludeer in B.J. Koops (2010), 'Cybercrime Legislation in the Netherlands', in: J.H.M. van Erp & L.P.W. van Vliet (eds), *Netherlands Reports to the Eighteenth International Congress of Comparative Law*, Antwerpen: Intersentia, p. 595-633, http://ssrn.com/abstract=1633958.

onvolkomenheden in de bestaande wetgeving die vanuit wetssystematisch oogpunt beter kunnen worden geregeld, waarvoor ik hierboven de nodige suggesties heb gedaan.
De 'snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit'[34] vragen om een voortdurende en voortvarende aanpassing van de wet, en de tijd lijkt dan ook rijp voor een Wet computercriminaliteit III. Voortvarendheid mag echter niet leiden tot haastwerk. Te hopen valt dat de wetgever de tijd neemt om zorgvuldig al het huiswerk dat voorvloeit uit de consultatie te verwerken, om een des te sterker wetsvoorstel aan het parlement aan te bieden ter versterking van de bestrijding van computercriminaliteit.

[34] MvT, p. 2.